Arizona Enterprise Architecture Target Technology Table		
Obsolete, Transitional	**Target (Strategic)**	**Emerging**
OSI Layer 1 – Physical		
Network		
Coaxial cabling, Category 3 unshielded twisted pair (UTP), shielded twisted pair (STP), and 62.5/125-micron multimode fiber	Category 5e UTP, Category 6 UTP 50/125 micron multimode fiber, 10/125 micron single mode fiber Structured cabling systems, based on TIA/EIA 568, 569, 606, 607 standards and applicable electrical codes	Wireless Infrastructureless, mobile “ad-hoc” networking Ultra-wideband (UWB) transmission
Bus topology	Logical star or mesh topology	Logical meshed topology
Security		
Open-door physical access	Keys, locks, badges, cameras, access logs, controlled access systems	IP-based access control systems, biometrics
Platform		
Platforms that employ proprietary protocols, gateways, as opposed to open-standard interfaces	SCSI, iSCSI	Trusted Platform
	Single application smart cards	Multi-function smart cards
OSI Layer 2 – Data Link		
Network		
Single-segment LANs, separate networks for different services (e.g., voice and data), separate dedicated networks for various user groups, proprietary protocols (e.g., SNA, Token Ring, Appletalk-addressing), FDDI, X.25, time-domain protocols (e.g., SDLC, HDLC)	Open, standards-based, multi-service networks 100 Mbps/1 Gbps/10 Gbps IEEE 802.3 Ethernet Wireless: IEEE 802.11 LAN, IEEE 802.16 MAN, IEEE 802.15 WPAN SONET, Frame Relay, ATM	Emerging packet- and cell-based wireless and satellite protocols 40 Gbps IEEE 802.3 Ethernet
Hub LAN technology	Switched LAN technology IEEE 802.1p/Q QoS, Diffserv, RSVP, VLAN, IEEE 802.3af PoE	
Security		
No Media Access Control Access Control Lists	Media Access Control Access Control Lists VPN Wireless: IEEE 802.11i, WPA, PEAP w/ IEEE 802.1x	
OSI Layer 3 - Network		
Network		
Proprietary protocols (e.g., IPX, AppleTalk-routing, DECnet) Fixed IP addressing	IPv4, IPv6 Routing Technologies: RIP, BGP, OSPF, IS-IS, MPLS, IGMP, PIM, MBGP DHCP	
Separate networks for different services (e.g. voice and data), flat designs with unmanaged bridges, hubs,	Converged networks with QoS, prioritization, and traffic flow control for all services, switched, multi-segment design Multi-layer switching Layer 3, wire-speed, network-level switching and prioritization	
Security		
Open, non-firewalled access Critical or Confidential data	Integrated firewalls - Packet filtering, ICMP Boundary Routers, end-point security, static NAT, IPSec	

Arizona Enterprise Architecture Target Technology Table		
Obsolete, Transitional	**Target (Strategic)**	**Emerging**
transmitted in clear formats		
OSI Layer 4 - Transport		
Network		
Proprietary protocols (e.g., SPX, AppleTalk-Transport)	TCP, UDP RTP, RTCP Converged networks with QoS, prioritization, and traffic flow control for all services Layer 4, wire-speed, transport-level switching and prioritization	
Security		
Open, non-firewalled access	Integrated firewalls - stateful inspection, dynamic NAT SSL, SSH	
OSI Layer 5 – Session		
Network		
AppleTalk-session and DEC-dns	DNS	Wire-speed, intelligent, session-level switching and prioritization
OSI Layers 6 – Presentation, 7 – Application		
Network		
AppleTalk-filing, and DEC-lat H.320	SNMP, RMON H.323, SIP with SDP, SAP, RTSP	Wire-speed, intelligent, content-level switching and prioritization
Security		
Open, non-firewalled Web, FTP, and Mail Servers Proprietary security products User selected passwords that do not conform to restrictive standards Signs-on's that only work with a single platform or application User-based privileges	Integrated firewalls - Application-proxy gateway, Proxy Servers, Dedicated Proxy Servers FTP, S/MIME for mail servers Encryption Technologies, PKI, OpenPGP, Smart cards, Kerberos Role-based administration, permissions, and rights Firewalled DNS, with services placed on DMZ Standards-based platform sign-on with role-based administration Industry-standard and vendor-neutral APIs for identification Strong password policy Token-based identification Public Key Certificates	Multi-function smart cards Enterprise directory services - LDAP meta-directory with an OID tree Single sign-on across platforms, domains Human Authentication API (HA-API) Public Key Infrastructure Mobile agents
Platform		
Platforms having proprietary operating systems without open-standard interfaces and drivers. For example:	Platforms having open industry-standard operating systems, with imbedded security, and open-standard interfaces and drivers Platforms having industry de facto standard operating systems, with imbedded security, and open-standard interfaces and drivers. For example:	Platforms having open industry-standard operating systems, with imbedded security, multifactor authentication, and open-standard interfaces and drivers

Arizona Enterprise Architecture Target Technology Table		
Obsolete, Transitional	**Target (Strategic)**	**Emerging**
o o Mainframes without TCP/IP o o Digital or analog PBXs /Key Systems requiring a separate network infrastructure o o Voice mail systems without open APIs o o Storage Area Networking with single-use, proprietary, fiber channel o o Pagers, used concurrently with PDAs, radios, cell phones o o Analog telephony devices	o o Mainframes with TCP/IP, SIP, Open APIs o o Servers with TCP/IP, SIP, Open APIs o o IP telephony with TCP/IP, SIP, H.323, ISDN PRI, open APIs, standard MOS codecs o o Hybrid IP telephony (TDM/IP) systems with TCP/IP, SIP, H.323, ISDN PRI, open APIs, standard MOS codecs o o Network Attached Storage o o Direct Attached Storage o o Storage Area Networking with multi-use access channels o o Client devices (PCs, Network Computers, PDAs, etc.) with wired/wireless connectivity, TCP/IP and multi-function applications	
Platform and Network Operating Systems that are unable to utilize a converged network infrastructure to access business applications	Platforms having niche proprietary operating systems, with imbedded security, and open-standard interfaces and drivers (requires exceptional business requirements) SNMP management of platforms Platforms deployed on target networks, with class of service (CoS) and quality of service (QoS)	
Software		
Traditional, monolithic State software applications deployed on proprietary server and client platforms (e.g., mainframe deployment requiring transitional version of OS with terminal access or terminal emulation access only, etc.)	n-tier distributed software applications emphasizing client (State employee, community of interest, public customer) productivity and performance enhancements and enablers (decision-making at the appropriate level) through self-service, self-administration, etc., utilizing browser-based (HTTP, HTTPS) client access deployed on Target Platform Architecture server, storage, and client devices Traditional, monolithic State software applications with web-enabled, browser-based (HTTP, HTTPS) client access	Open, industry standard Web services, .NET, WSDL, XML, UDDI initiatives Software applications hosted via ASPs
Client/server software applications deployed with “fat” client requirements	Three-tier distributed software applications with access to n-tier architecture services	
Business programming languages such as COBOL used in legacy software applications Manufacturer-specific programming languages Platform-specific programming languages such as assembler, etc.	C++, Java™, Visual Basic®, etc.	
Proprietary gateways, interfaces DCE Vendor/database-specific middleware with proprietary extensions	Java™ and servlet software, COM™, DCOM™ CORBA, ORB, ISO/IEC 11179 Open API Middleware: TPM, RPC, RMI, JMS, MOM HTML, XHTML, XML	Object-oriented software IIOP J2EE™ EJB™ server-side deployment, COM+ EbXML secure exchange of information, UML™, SAML, XSL, CSS3, XSLT, DSML, SOAP, TLS

Arizona Enterprise Architecture Target Technology Table		
Obsolete, Transitional	**Target (Strategic)**	**Emerging**
3270 terminal access to software	GUI presentation layer access to software as a precursor to browser-based (HTTP, HTTPS) access Browser-based (HTTP, HTTPS) access to software	Portal-based universal browser access to all services
Unmanaged software applications	Software applications that are manageable with SNMP-based management tools	Enterprise federated management
	LDAP directory services	Enterprise LDAP directory services
	Software application security	
Flat file systems, ISAM, VSAM	RDBMS	OODBMS, ORDBMS
Vendor-specific SQL extensions	Open database connectivity: SQL, ODBC, OLE DB, NDMP, NFS, CIFS, JDBC	
Vendor-specific database middleware with proprietary extensions	Database middleware that uses open database connectivity	
Proprietary email systems, non-MIME-compliant email, proprietary, closed email directory services	Email services: SMTP, S/MIME, IMAP4, POP3	Enterprise email directory services
Proprietary, closed productivity software	Productivity software with open APIs	Productivity software conforming to IETF standards such as iCalendar, CAP, IPP, etc.

The terms "Obsolete, Transitional, Target (Strategic), and Emerging" as defined herein provide guidance regarding the status of specific architecture technologies. Deployment and implementation of Enterprise Architecture Target Technologies shall be in accordance with *Statewide Policy P700, Enterprise Architecture,* and *Statewide Policy P340, Project Investment Justification (PIJ).* Additional guidance and information is available in domain-specific, statewide policies and standards. Please refer to http://gita.state.az.us/policies_standards for the most current versions of policies and standards.

- **Obsolete.** Arizona's EA strongly promotes that agencies employ a different technology. Agencies must not plan new deployments of this technology and should develop a plan to replace this technology. This technology is typically outdated, no longer widely supported by the original manufacturer, and has been superseded by a newer, better technology.
- **Transitional.** Arizona's EA promotes other standard technologies. Agencies may presently be using this technology as a transitional strategy in movement to a target/strategic technology. This technology may be waning in use by industry or no longer supported by the original manufacturer.
- **Target (Strategic).** Arizona's EA promotes use of this technology by agencies. Deployments of all target technologies should be the most currently available (having widespread, mainstream adoption and implementation by industry) and supported (by the original manufacturer) version of the technology.
- **Emerging.** Arizona's EA promotes only evaluative deployments of this technology. This technology may be in development or may require further evaluation.

October 17, 2003